



„Next Generation Firewall” (NGF) kontra „Unified Threat Management” (UTM)

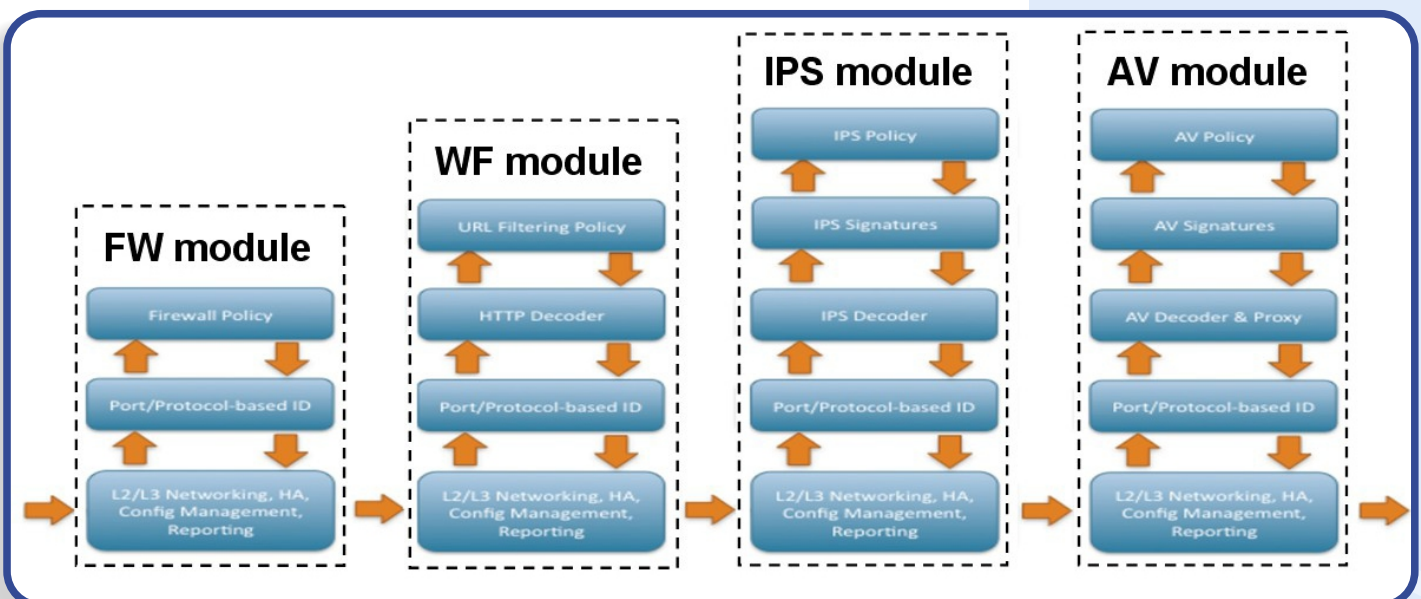
Wstęp

System Firewall jest najbardziej istotnym elementem infrastruktury bezpieczeństwa sieciowego każdej firmy. Jest to system, który jest (a przynajmniej powinien być) instalowany w pierwszym rzędzie - wraz ze stałym łączem internetowym. Wybór systemu firewall jest więc dla każdego przedsiębiorstwa decyzją strategiczną, niezależnie czy na jego zakup decyduje się mała firma rodzinna czy też wielka korporacja.

W niniejszym dokumencie przedstawiamy podstawowe różnice pomiędzy systemami firewall lasy **UTM** a **NGF**. Wyjaśniamy różnice w architekturze sprzętowo-programowej oraz ich konsekwencje w praktycznych wdrożeniach systemów bezpieczeństwa.

UTM a NGF - definicje

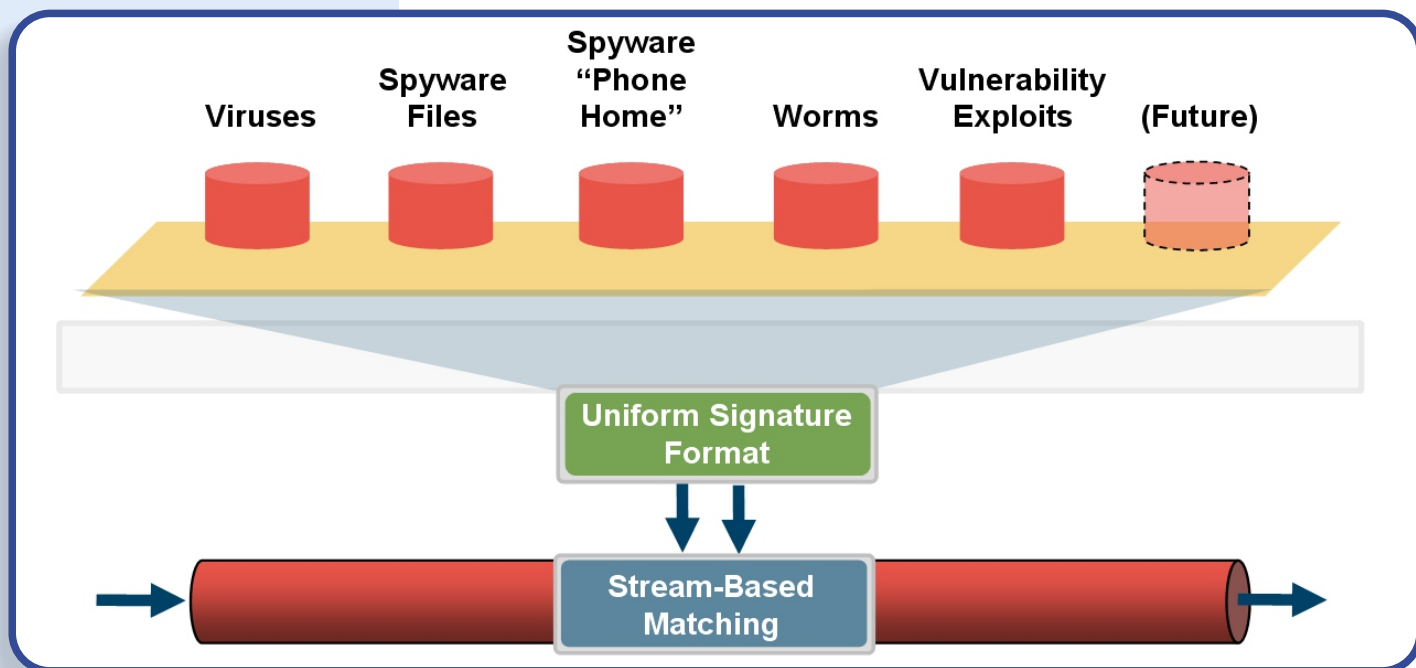
System **UTM** - to „klasyczny” firewall bazujący na filtracji ruchu zgodnie z zasadą „stateful inspection” (SPI) opracowaną przez firmę CheckPoint w połowie lat 90-tych, a obecnie implementowaną w przeważającej większości systemów firewall. W skrócie - metody SPI filtracji ruchu polega na kontrolowaniu przez firewall strumieni TCP oraz logicznych sesji UDP w taki sposób, aby tylko pakiety „pasujące” do zdefiniowanych reguł bezpieczeństwa były przepuszczane przez firewall (pozostałe zaś blokowane). W systemie UTM podstawowy moduł SPI rozbudowany jest o dodatkowe moduły realizujące kontrolę danych; są to: moduł antywirusowy (AV); moduł antyspam (AS); moduł filtracji adresów URL (URLF) oraz moduł wykrywania ataków IDS/IDP.



Rysunek 1 - architektura systemu UTM - każdy z modułów filtracji działa niezależnie dokonując odpakowania i inspekcji danych.

Firewall typu UTM operuje więc na polityce bezpieczeństwa zdefiniowanej na podstawie reguł opisujących dozwolony ruch: „skąd-dokąd” - na poziomie adresów IP, adresów DNS oraz portów sieciowych. Dla wybranych protokołów, takich jak HTTP, FTP, SMTP, POP, IMAP może być realizowana inspekcja danych.

Sprzętowo firewall UTM może realizować całą filtrację ruchu na jednym procesorze lub dedykować do poszczególnych modułów (np. AV czy IDP) osobne procesory lub rdzenie; należy jednak zwrócić uwagę na bardzo istotny fakt: w systemach UTM moduły pracują niezależnie od siebie i niezależnie od głównych funkcji firewall-a - są „klockami” dołożonymi do podstawowej funkcjonalności systemu filtracji SPI - firewall typu UTM jest więc rozszerzeniem klasycznego firewall-a SPI.



Rysunek 2 - architektura systemu **NGF** - filtracja danych odbywa się poprzez jeden system dopasowania reguł.

System **NGF** podobnie jak UTM realizuje funkcje inspekcji danych; jednak w przeciwieństwie do UTM funkcje te realizowane są w ramach jednego uniwersalnego modułu inspekcji danych, tj. jednego zestawu sygnatur filtracji. Tak więc cała filtracja danych realizowana jest w spójny sposób na jednym poziomie stosu sieciowego. Jednocześnie filtracja może być realizowana na wielu (dedykowanych) procesorach w celu zapewnienia odpowiedniej wydajności.

Różnice funkcjonalne

W zakresie powierzchownie porównywanych cech różnice funkcjonalne pomiędzy UTM a NGF są niewielkie: obydwa rozwiązania realizują skanowanie antywirusowe, wykrywają próby włamań, itp. Różnica tkwi jednak w dokładności klasyfikacji oraz precyzji konstruowania reguł: system UTM nadal operuje w dziedzinie adresów i portów. System NGF operuje w warstwie aplikacji, co pozwala np. na zablokowanie przesyłania danych w protokole Skype lub wyłączenia dostępu do gier na portalu Facebook (ale nie do samego Facebook-a). Niektóre systemy UTM w pewnym zakresie mogą realizować podobną filtracją danych,

jest ona jednak zintegrowana w zestaw głównych reguł polityki bezpieczeństwa - co utrudnia administrację. Jednak, co ważniejsze filtracja danych poprzez wydzielony moduł IPS w UTM odbywa się dużo mniej wydajnie niż w NGF.

Wydajność

Przypomnijmy: Podstawowym problemem każdego UTM jest konstrukcja sprzętowa. Każdy UTM to historycznie moduł firewall, do którego później zostały dodane kolejne moduły jak Intrusion Prevention (IPS), Anty-Wirus (AV) i URL Filtering. Nie ma przy tym znaczenia, że funkcje UTM będą wykonywane na jednym czy wielu bladach (CPU czy core-ach).

Widać to bardzo wyraźnie w specyfikacjach producentów. Przykładowe urządzenie UTM jednego z producentów posiada wydajność 7 Gbps dla samego modułu Firewall, 4 Gbps dla firewall i włączonego modułu IPS oraz zaledwie 500 Mbps dla firewall i modułu AV - samo włączenie AV (wg. danych producenta, które mogą być zawyżone) powoduje degradację wydajności aż 14 razy. Włączenie IPS dodatkowo obniży wydajność, włączenie filtracji URL jeszcze bardziej, itd.

Żaden producent UTM nie podaje ile wynosi wydajność urządzenia zabezpieczeń przy włączonych wszystkich funkcjach ochrony. Na podstawie testów UTM wykonywanych u operatorów w Polsce wiemy, że jest to degradacja wydajności rzędu 30-50 razy! Z tych powodów z założenia UTM nie nadaje się do zastosowań u operatorów telekomunikacyjnych, w centrach danych, w sieciach wewnętrznych i wszędzie tam gdzie wydajność zabezpieczeń ma krytyczne znaczenie.

Dla produktów NGF włączenie pełnej inspekcji danych, tj. funkcji AV, IDP, itp. powoduje zmniejszenie wydajności o 2-4 razy w stosunku do maksymalnej wydajności samego urządzenia firewall. Przy czym dodać należy, że są to faktycznie zmierzone wartości w środowiskach produkcyjnych, a nie tylko podawane przez producenta wyniki testów laboratoryjnych.

W roku 2009 pojawił się raport Gartner wykonany na podstawie analizy działania w amerykańskich firmach różnych rozwiązań firewall, IPS i UTM - załącznik *Gartner-NGFWResearch-Note.pdf*. Raport wyraźnie wskazuje na konieczność przebudowania "starych" rozwiązań firewall/IPS/UTM w kierunku tzw. Next-Generation Firewall (NGF).

Bezpieczeństwo Sieci



Oferujemy systemy NGF i UTM następujących producentów:

- Check Point Technologies,
- Fortinet,
- Juniper Networks,
- Palo Alto Networks,
- McAfee.

JUNIPER
NETWORKS

paloalto
NETWORKS



Check Point
SOFTWARE TECHNOLOGIES LTD.



Kiedy system UTM a kiedy NGF?

Przed rozpoczęciem wyboru producenta systemu firewall powinniśmy przygotować następującą (lub podobną) tabelkę:

<ul style="list-style-type: none">• Całkowita liczba użytkowników w centrali i ew. oddziałach• Liczba użytkowników w centrali i oddziałach (osobno)	_____ _____
Czy i jakie funkcje skanowania danych są potrzebne: Antywirus, antyspam, IDS/IDP, filtrowanie URL	AV: AS: IDS/IDP: URLF:
Czy skanowany jest tylko ruch wchodzący i wychodzący do Internetu czy także ruch wewnętrzny	[TAK] [NIE]
Jaka jest wymagana całkowita zagregowana przepustowość systemu firewall przy włączonych funkcjach skanowania	[TAK] [NIE]
Jakie są wymagania na liczbę i typ interfejsów (np. wymagania odnośnie interfejsów optycznych: SFP, SFP+, XFP, itd.	
Inne wymagania: integracja z domenów Windows, wirtualizacja, itp.	[TAK] [NIE]

Dostępne rozwiązania

Poniżej podsumowaliśmy najważniejsze cechy oferowanych przez nas rozwiązań NGF i UTM:

Producent	Typ	Cechy
PaloAltoNetworks	NGF	„Prawdziwy” system NGF ze sprzętowym wspomaganie filtracji, rozdzielonymi ścieżkami danych i sterowania; reguły aplikacyjne w pełni zintegrowane w zestaw reguł filtracji. Nie posiada modułu <i>AntySpam</i> . Dostępne w postaci systemów appliance.
CheckPoint	NGF/UTM	System UTM z modułem NGF; wersje appliance oraz oprogramowanie na serwery PC
Juniper SRX	UTM	appliance ze sprzętowym wspomaganie filtracji (w większych modelach); wymaga osobnego systemu zarządzającego do pełnej obsługi funkcji IDP
Juniper SSG	UTM	Klasyczny system UTM appliance

Wybrane referencje CC w zakresie rozwiązań firewall i ochrony danych:

- Agencja Mienia Wojskowego
- Biuro Trybunału Konstytucyjnego
- Bank BPS S.A.
- Bank Handlowy S.A.,
- Bank Millennium S.A.,
- Coffee Heaven Sp. z o.o.
- Exatel S.A.
- Ferrero Polska Sp. z o.o.
- Gielda Papierów Wartościowych S.A. w Warszawie
- Instytut Badań Systemowych PAN
- Krajowe Biuro Wyborcze
- Instytut Geofizyki PAN
- Narodowe Centrum Badań Jądrowych
- Ministerstwo Sprawiedliwości,
- Opera TFI S.A.
- Provident Polska S.A.,
- Sodexo Polska Sp. z o.o.
- Polski Bank Przedsiębiorczości S.A.
- Sodexho Pass Polska Sp z o.o.
- Ubezpieczeniowy Fundusz Gwarancyjny
- Uniwersytet Warszawski
- Unicredit CA IB S.A.
- UPC Telewizja Kablowa

Więcej informacji o firmie znajdziecie Państwo w Internecie, na stronach:

<http://www.cc.com.pl/>

Kontakt:

Dział Techniczny: tech@cc.com.pl

Dział Handlowy: sales@cc.com.pl

Bezpieczeństwo Sieci

